Unclassified

A Continuing Need for Protection

Legislative and Judicial Safeguards for US Intelligence Personnel (U)

(b)(3)(c)

Remember Phil Agee, who I consider a traitor to our country? The guy encouraged the publishing of names of those serving under cover, sacrificing their lives. And Counterspy *magazine did publish names, including the name of Richard Welch, our station chief in Greece, who shortly thereafter was gunned down in Greece outside his residence.(1)*

Former President George Bush

17 September 1997

Former President and Director of Central Intelligence (DCI) Bush's mention of Philip Agee, the former Directorate of Operations (DO) officer turned traitor, was made to retirees attending festivities at CIA Headquarters recognizing the Agency's 50th birthday. It also coincided with the 15th anniversary of the enactment of the Intelligence Identities Protection Act of 1982 (IIPA), legislation that was created partly in response to Agee's activities.

On 23 December 1975, Richard Welch was shot down near his residence in Athens(2) by three gunmen shouting in Greek.(3) Following the murder, DCI William Colby revealed that Welch, ostensibly a First Secretary at the US Embassy, was a CIA employee.(4) A previously unheard of terrorist group, the Revolutionary Organization 17 November, claimed responsibility for the killing.(5)

The incident provoked widespread examination of both the quality of cover for American intelligence officers(6) working overseas and of the activities of Americans who purposely engaged in exposing the identities of clandestine operatives. With respect to the former, Welch had lived in the same house as his CIA predecessors, and he was not listed in the State Department's biographical book of senior diplomatic personnel.(7)

Equally important, Welch had been fingered in *Inside the Company: A CIA Diary*, the 1975 book written by Agee that detailed hundreds of alleged officer identities. In addition, Welch had been named as a purported CIA employee in an article printed in the Washington quarterly *Counterspy*, a publication supported by a group of disaffected former intelligence officers who called themselves "The Fifth Estate." Agee served on *Counterspy's* advisory board.(8) The contents of the *Counterspy* article were in part reprinted in an English-language publication entitled *Athens News*. The Greek piece went so far as to include both Welch's address and telephone number. Once Welch had been identified publicly in Greece, members of 17 November simply needed to wait outside his home in order to ambush him.(9)

More Accusations

After Welch's death, the editors of *Covert Action Information Bulletin*, a leftwing publication that

continues in print, visited Kingston, Jamaica, and Maputo, Mozambique. In Kingston, the "journalists" held a news conference at which they claimed that 14 American Embassy employees were spies and provided the officials' addresses, telephone numbers, and the license-plate numbers and colors of their automobiles. Within 48 hours, the residence of one official had been raked by submachinegun fire and an explosive device detonated, causing extensive damage. A few days later, a separate attempt apparently was made to kill another of the alleged intelligence officers.(10)

Following the visit to Mozambique by *Covert Action's* staff, a Cuban Counterintelligence (CI) team arrived in Maputo. The Cubans forcibly detained an American diplomat there and offered him a sizable sum of money to spy for Havana. Mozambique subsequently declared the diplomat, three other Embassy officials, and two wives *persona non grata*.(11) Three months later, one of the four officials expelled from Maputo was PNG'd from Zambia, amid similar allegations of being a CIA employee.(12)

The IIPA

The various hostile actions against US intelligence officers gave impetus to the efforts to enact legislation aimed at punishing those who sought to expose their identities. In 1982, after protracted legislative wrangling, the final text of the IIPA was signed into law at CIA Headquarters by President Reagan, who said "...the enactment of the Intelligence Identities Protection Act is clear evidence of the value this nation places on its intelligence agencies and their personnel."(13)

The legislation provides for three criminal penalties:

- Section 421(a) applies to those who have had access to classified material that identifies a "covert agent" and who intentionally disclose the identity knowing that the United States is trying to protect the identity of the agent and that the beneficiary is not authorized to receive classified information. For purposes of the entire act, a "covert agent" is a US intelligence officer who has served overseas within the past five years; a US citizen (a source) who is either residing overseas providing Foreign Intelligence (FI) or CI to a US intelligence agency or residing domestically and providing FI or CI to the FBI; or a non-US citizen (an asset) whose prior or present relationship with the US Government is classified. The penalty under 421(a) is a fine of up to $50,000, not more than 10 years in prison, or both.

- Section 421(b) is identical to 421(a), except that it applies only to those who in the course of authorized access to classified material discovered an agent's identity and disclosed it. The penalty is a maximum fine of $25,000, not more than five years in prison, or both.

- Section 421(c) states that, "Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States," discloses the identity to an individual not authorized to receive classified information will be fined no more than $15,000, will serve no more than three years in prison, or both. It is important to note that under 421(c), unlike either 421(a) or 421(b), the disclosing individual need not have had access to classified information.

- In addition to the IIPA's three crimes, Section 423(a) mandates that the DCI submit to the House and Senate intelligence oversight committees, "an annual report on measures to protect the identities of covert agents, and on any other matter relevant to the protection of the identities of covert agents." Although reports were submitted in 1983 and 1984, available information indicates that since 1985 no such account has been sent to Congress.

Section 421 (c) predictably was of great concern to civil libertarians. Some posited that an American citizen could be imprisoned for independently investigating intelligence entities and disclosing the names of covert agents. There also was consternation over the "reason to believe" standard that governed to what degree a violator had knowledge that he was impairing US intelligence activities. Law review articles and public debate were spawned from what was bemoaned as an unacceptable encroachment on the First Amendment at the height of the Cold War.(14)

Despite such concerns, the IIPA has been largely dormant. This is especially true for IIPA's clause to prosecute those who have never had access to classified information, the very part of the Act that was the target of the overwhelming majority of its critics.

Two Convictions

Since the Act's passage, only two individuals have been convicted under its auspices: CIA employee Sharon Scranage and US Marine Sgt. Clayton Lonetree. Scranage was stationed in Accra, Ghana, in the early 1980s. She had an affair with a purported businessman who, as a cousin of Ghana's head of state, had been tasked with penetrating the CIA's operations in Ghana. Scranage revealed the identities of a number of assets to her lover, resulting in severe damage to the CIA's equities in Ghana.(15)

Scranage was charged with 18 criminal counts, including espionage charges. Under a deal brokered with prosecutors, she pled guilty to only two counts under Section 421(a). Although Scranage initially was to serve five years in prison, her sentence later was reduced to two years with an opportunity for release after 18 months.(16) The case is an example where the Act was used as a shotgun litigation approach, in which Scranage was given room to acknowledge her failures in return for a lesser penalty than would have accompanied an espionage conviction.(17)

Lonetree was also convicted under the IIPA. He aided the Soviets while detailed to Marine Security Guard detachments at US Embassies in the Soviet Union and in Austria.(18) Besides revealing details of American activities in Moscow, Lonetree also admitted to disclosing the identities of intelligence officers serving in the US Embassy in Vienna.(19) He was charged with violating the IIPA, in part because under the military justice system all potential charges arising from a particular incident have to be presented at the same time. This is in contrast to civilian courts, where, though a defendant may be found not guilty of a charge stemming from the incident involving alleged criminal conduct, prosecutors may subsequently try the defendant again on other counts. In any event, Lonetree was convicted on a host of violations of the Uniform Code of Military Justice, including a General Article incorporation of Section 421(b) of the IIPA.

Neither conviction was particularly significant. Both Scranage and Lonetree were subject to other criminal charges. If IIPA had not existed, both still would have been incarcerated for their treason.

Deterrent Effect

The IIPA, especially section 421(c), has had some positive impact. *Covert Action Information Bulletin* no longer focuses on uncovering identities. And Philip Agee has stated his intention to abide by the law. According to press reports attributed to a former officer in Cuban intelligence, Agee was for years a paid agent of Havana. A vocal opponent of the US Government, the Cubans purportedly fed him his lines.(20) He reportedly also instructed Nicaragua's Sandinistas on how to detect US intelligence personnel and tried to recruit a member of the US Embassy in Mexico City under the guise that he still worked for the CIA.(21)

After the Department of State revoked Agee's passport privileges in 1979, he began using a Grenadine passport. Since then, he evidently has been using a passport issued by Germany, his wife's native country. Agee reentered the United States in 1987 after 16 years abroad, and he continues to visit America for speaking engagements. In 1987, Agee insisted, "I never regretted, and still don't, naming the names of agents and exposing the operations" but that, in reference to the IIPA, "I don't think that there's any need to break the law."

Statutory Burden

To prosecute a member of the media under Section 421(c), the Department of Justice (DOJ) would have to prove beyond a reasonable doubt that the news organization was engaged in "a pattern of activities

intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States."(22) The IIPA categorically exempts investigations of intelligence failures and journalists. According to the Senate Judiciary Committee report on the IIPA:

> *A newspaper reporter, then, would rarely have engaged in a pattern of activities with the requisite intent to "uncover" and "expose" covert agents. Instead, such a result would ordinarily be "the (anticipated) side effect of his conduct". . . . To meet the standard of the bill, a discloser must be engaged in a purposeful enterprise of revealing names--he must, in short, be in the business of "naming names."(23)*
>
> *According to the Act's sponsor, Senator John Chafee of Rhode Island: We have carefully differentiated between the journalist who may reveal the name of an agent in a news article and the person who has made it his purpose and business to reveal the names of agents, and has engaged in a pattern of activities intended to do so. Clearly, the legitimate journalist would not be engaged in such a pattern of activities.(24)*

The limited extent of the IIPA is perhaps best summed up by the House-Senate Conference Committee report, which states that the Act:

> *. . .does not affect the First Amendment rights of those who disclose the identities of agents as an integral part of another enterprise such as news media reporting of intelligence failures or abuses, academic studies of US Government policies and programs, or a private organization's enforcement of its internal rules.(25)*

This high standard effectively restricts the IIPA's clauses to two classes of individuals: outright traitors, who, in any event, are subject to concurrent espionage charges; and those who clearly espouse an interest in harming the Intelligence Community (IC) and have engaged in a consistent pattern of behavior to accomplish their goal. Going beyond these two circumscribed categories violates both the Act's express burden and its purpose as enunciated by Congress.

Establishing a "pattern" is intellectually tricky. If an individual reveals identities and has done so before, but adds cushioning language such as calling for a criminal or Congressional investigation, is that individual guilty of trying to impair foreign intelligence activities? Or is the individual simply an intelligence critic? Where is the line drawn between investigator and miscreant? As a matter of practicality, journalists with mainstream publications or academics at distinguished institutions are not apt to be labeled the latter.

The government also has to prove beyond a reasonable doubt that the perpetrator had "reason to believe" that his or her activities would impair or impede US intelligence programs. This criterion originally was opposed by civil libertarians because it did not require a suspect to have concrete premeditation or intent to harm US intelligence activities. Nonetheless, the "reason to believe" standard is problematic because it turns the trial into a subjective inquiry into whether the defendant had "reason to believe." Many defendants would maintain that under no circumstances did they presume that they were harming US intelligence capabilities.

At times, the DOJ has been accused of being timid in seeking IIPA prosecutions. In the conference committee report for the 1997 fiscal year intelligence appropriations bill, Congress admonished that, "The conference report expresses the sense of Congress that the DOJ be more forceful in enforcing the Intelligence Identities Protection Act, which was a provision strongly supported by the House."(26) Such a direct apparent censure of DOJ is noteworthy because Congress's language in establishing the IIPA and the statute itself ties DOJ's hands. Congress's 1997 decree also could have been meant to provide explicit recorded guidance for DOJ to be more aggressive in seeking IIPA charges. The budget statement certainly demonstrates there is at least some degree of political will to address more actively the issue of exposed covert identities.

Practical Obstructions

Despite Section 421's textual constraints, the CIA does refer matters to the DOJ for investigation. With Section 421(a) and (b) violations, there are procedural impediments inherent in any investigation of an unauthorized disclosure. The information may have been disseminated to a large number of individuals. The DOJ or the FBI also may deem that the disclosure is not sufficiently damaging to justify expending the resources for a prosecution. Section 421(c) violations are somewhat less susceptible to the procedural obstacles of Section 421 (a) and (b) violations because pinning down who revealed the identity usually is a less arduous exercise.

Another Act

Nonetheless, Section 421(c) prosecutions remain difficult because the American tradition of public courts does not accord well with trials involving classified information. The Classified Information Procedures Act (CIPA)(27) provides a statutory rubric for reconciling a constitutionally enshrined open-court system with the need to protect sensitive national security information. Of particular interest in CIPA is Section 6(c), entitled "Alternative Procedure for Disclosure of Classified Information." In short, the Act authorizes courts to substitute a summary or subset of facts of certain classified information in lieu of the complete text which otherwise would have been disclosed at trial. For example, instead of revealing the contents of an entire report, the government could merely present a summary of particularly key information within it. CIPA involves two sets of rulings by a judge: an *ex parte* decision regarding what the defense counsel may see; and a subsequent determination of what actually will be presented at trial, as argued by both the prosecution and the defense. If, after the first decision, the prosecution refuses to turn over sensitive material to the defense, the judge may dismiss the case.

CIPA's Section 6(c) was refined by the common law creation of what has become known as the silent witness rule. The procedure allows a witness to point to classified information on papers which the prosecution, defense counsel, defendant, judge, and jury all possess, rather than having the witness respond orally. The aforementioned parties also may don headphones to hear testimony. In this manner, classified material is kept from the public record. Under CIPA and case law, the defense counsel may be required to be security screened for access to classified material; the jury, however, cannot be security cleared. Furthermore, the judge has the discretion to determine what material may be eligible for substitution, if the silent witness rule may apply, and the degree to which court records will be sealed.

Thus, there is an inherent uncertainty in any IIPA prosecution as to what extent an identity will have to be confirmed by the government in the course of a criminal proceeding. The CIA may be reluctant to acknowledge an intelligence identity in court for the very reasons that the CIA does not wish identities to become public in the first place. A report often may contain a number of alleged identities, some of which are incorrect. By confirming what is accurate, the CIA is forced to separate publicly what may be a few grains of wheat from a significant amount of chaff. As a result, trials hold the potential for being more damaging than the initial disclosure. The CIA consequently is left with an unpleasant dilemma: confirming an identity may further risk sources and methods, but refusing to prosecute the offender de facto encourages similar disclosures in the future.

A remedy to the problem could be to tighten CIPA to force judges to seal all court records involving classified information and to issue instructions, on penalty of being imprisoned for contempt of court, that no court personnel or member of the jury should disclose or discuss the identity outside of the courtroom. Staunch civil libertarians perhaps would object to such a measure as further eroding the Sixth Amendment's guarantee to a public trial. Such a revised rule for CIPA would merely extend CIPA one step further on intelligence identities, a narrowly tailored area in which the government has an overwhelmingly compelling state interest. It would not security-screen jurors or otherwise tamper with the jury system; jurors would remain free to speak about information not directly related to the identity of a covert officer, source, or asset or information otherwise restricted under CIPA.

Judges could object to these proposals on the constitutional grounds that Congress was interfering with

the separation of powers. Such criticism is mitigated by the fact that the judges would be free to decide what evidence would be admissible. The restrictions would be limited to deciding who beyond the jury and counsel heard the material. This is an administrative determination that neither infringes on the independence or integrity of the court, the key criteria set forth in *Mistretta v. United States* (488 U.S. 361 [1988]), in which the Court validated the Congressionally imposed system of sentencing guidelines.

Section 421(c)'s problems regarding having to make inadvertent disclosures in open courts in order to obtain convictions brings the analysis full swing back to Sections 421(a) and (b) because courts traditionally have held that employees or others who enjoy access to classified material may contractually waive legal rights. If an intelligence officer may sign away his First Amendment right to free speech, then cannot the same officer also contract away his Sixth Amendment right to a public court?

A Secret Court System

Such an argument is made all the more interesting by recent developments in establishing the first quasi-adversarial, secret civilian court system in America, the Alien Terrorist Removal Court (ATRC). The ATRC is authorized under the aegis of the Federal Anti-Terrorism and Death Penalty Act of 1996. Its mission is to determine whether the United States may deport lawful permanent resident aliens and other noncitizens suspected of involvement in terrorist activities.

To understand the ATRC first requires examining the advent of secret courts with special jurisdiction. This type of judicial body was the direct consequence of the Foreign Intelligence Surveillance Act of 1978 (FISA), which authorized the establishment of a small and shrouded Federal court to entertain warrant applications for electronic surveillance of agents of foreign powers located within the United States.28 The Act was in amended in 1994 to include physical searches, the pursuing of warrants for which was then authorized in 1995 by President Clinton under Executive Order 12949.(29)

The FISA Court is composed of seven district court judges appointed by the Chief Justice who sit for seven-year terms and who periodically travel to Washington to hear FISA applications. In the event a petition is denied, a special three-judge appellate panel appointed by the Chief Justice and drawn both from district courts and appellate circuits may invalidate the initial warrant decision and authorize the surveillance operation. If such a reversal is made, the written decision is dispatched to the Supreme Court, which has the power to review it.

As FISA exclusively examines warrant applications, no defense counsel or defendants are present. The court sits in a classified environment, and its records remain under seal and are protected by strict security standards. Court personnel, including judges, are subject to security screening by the FBI.(30)

For nearly two decades, FISA stood on the cutting edge of the division between the need for national security and an open-court environment. The Act was tapped during the investigations of Ames and of convicted former FBI agent Earl Pitts. The court has never turned down a government warrant request, which means the appellate mechanism has never been used. FISA judges have, however, annotated warrant applications or advised that they be resubmitted in a revised format.(31) The Act has never been challenged in court, save for fleeting arguments by former CIA employee Harold Nicholson that FISA was unconstitutional. Nicholson subsequently chose to plead guilty to espionage charges and received a reduced sentence of 23 years, seven months, rather than pin his hopes for ever gaining freedom on the Act's alleged flaws.

The ATRC

FISA's ability to anger civil libertarians was partially usurped in 1996, when Congress introduced the ATRC, which is equally as secret as FISA but which encompasses an area of the law that previously entailed a public adversarial process. Although as early as 1998 no case had yet to be presented to the ATRC, extensive preparations have been made to establish its procedures. The court is composed of five district court judges selected by the Chief Justice for five-year terms who sit in Washington when

hearing associated cases.

Under the Anti-Terrorism Act and procedures promulgated by the ATRC's presiding Chief Judge, judges hear classified evidence in an *ex parte* proceeding that includes specially cleared defense counsel but not the defendant. This is an unprecedented departure from traditional criminal procedure. Under the ATRC, a "special attorney," drawn from a discreet list of previously cleared counsel, would *in camera* defend his client but is prohibited by statute from subsequently sharing the substance of the proceedings with that client. This creates a trial with a de facto defendant in absentia, albeit only a room away. Unlike FISA, which established a separate appellate panel, the ATRC's appeal is handled under seal and *ex parte* by the United States Court of Appeals for the District of Columbia Circuit.

Although the ATRC is nominally "public," the court in reality is secret. Evidence may both be presented and remain under seal without opportunity for examination by the defendant or admission into the public record. The ATRC's constitutional justification is that the potential damage from revealing intelligence sources and methods to the defendant is so grave and the penalty of exclusion of a noncitizen from the United States so minor that the amount of secrecy in ATRC's quasi-adversarial proceedings is allowable. The ATRC is a major step toward addressing the need to protect sensitive national security information during a trial.

If the ATRC is upheld as a constitutionally permissible means of conducting a court proceeding, an argument is to be made that IC employees, including staff members of the Congressional oversight committees, should be subject to similar secret courts pursuant to their employment contracts. This line of reasoning can be taken one step further to advocate a similar closed court for American citizens who are not members of the IC but are accused of violating Section 421(c). Although the latter could foreseeably be politically untenable, a closed court for IC employees would be similar in principle to the military justice system. Americans could avoid being prosecuted in the secret IC court by simply not joining the IC, just as Americans may currently avoid prior restraint by not becoming employed by the IC. A secret IC court system would dramatically reduce the practical problems inherent in prosecuting unauthorized disclosures.

Prior Restraint Controversy

The issue of prior restraint, in which the government would be able to exercise prepublication review over the media, is another subject of heated controversy. There is a plausible argument that a government censor should have access to prepublication proofs of articles that may reveal identities, but the mere mention of this sort of system provokes cries of an Orwellian repression of the media.

As the Supreme Court noted in *Near v. Minnesota* (283 U.S. 697 [1931]), reports on troop and transport unit movements are not protected by the First Amendment. Most hopes for prior restraint, however, were jettisoned in the aftermath of *The New York Times v. United States* (403 U.S. 713 [1971]), the 6 to 3 landmark decision which declared that the government could not censor *The New York Times* when the newspaper proposed to publish *The Pentagon Papers*, a 7,000-page compendium of leaked classified analyses. As Chief Justice Burger pointed out in his dissent, however, the case is susceptible to much criticism. The decision was hasty, bypassing the normal route of district and appellate findings. Burger quoted Holmes in *Northern Securities Co. v. United States* (193 U.S. 197 [1904]):

> *Great cases like hard cases make bad law. For great cases are called great not by reason of their real importance in shaping the law of the future but because of some accident of immediate overwhelming interest that appeals to the feelings and distorts the judgment. These immediate interests exercise a kind of hydraulic pressure that makes what previously was clear seem doubtful, and before which even well settled principles of law will bend.*

The "hydraulic pressure" in *The New York Times* was the public's distrust of the Vietnam policies of various administrations. To have prevented publication of the papers would only have increased that distrust. This case remains the controlling one for prior restraint.

That said, prior restraint does not have to entail unilateral government censorship. The DOJ could request an injunction against publication of certain identities and refer the matter to a court using CIPA procedures where the reporter and publisher would receive a fair hearing.

The United States would not be alone in censoring publications. The UK's Official Secrets Act of 1911 rigorously controls the dissemination of classified information and has led to a vigorous system of prior restraint. Israel has an active censorship system for military and intelligence affairs. Both France and Germany have laws authorizing prior restraint. Limiting prior restraint in the United States to intelligence identities (or even classified analyses) would be a narrower schematic for restricting speech than exists even in these democracies. Furthermore, in past cases where the United States Government has known that the publication of an identity is forthcoming, prior restraint would have been useful.

A Continuing Concern

Despite the end of the Cold War, intelligence personnel remain at risk in many parts of the world. In the past few years, several significant terrorist actions were taken against official Americans:

- In 1993, Mir Aimal Kasi opened fire on CIA employees waiting in vehicles to enter CIA Headquarters in Langley, killing two.
- In 1995, three employees of the US Consulate in Karachi, Pakistan, were gunned down at a traffic intersection. Two died.
- In 1996, 19 US military personnel were killed in the bombing of the Khobar Towers barracks in Dhahran, Saudi Arabia.
- In 1996, 17 November carried out a rocket attack on the US Embassy compound in Athens. In all, 17 November allegedly is responsible for murdering four Americans and injuring 28 . Media reports indicate that the same .45-caliber pistol that killed Welch was used in the June 1997 assassination of a Greek shipping tycoon. No member of 17 November has ever been caught.(32)
- In 1998, the bombings of the US Embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, resulted in the deaths of 12 Americans.

In addition, the advent of the World Wide Web carries with it extraordinary opportunities to unearth covert identities. Using a web-search agent, electronic sites may be scoured in seconds. For a fee, one may access and cross-index articles from thousands of domestic and foreign publications going back to the seventies. A one-time disclosure of an identity in even an obscure periodical is easily traced in this manner. While such an approach may be expensive for the average individual, it is a simple exercise for a foreign intelligence service or a reasonably sophisticated terrorist group.

For example, as a test, a commercial database was accessed and searched for the classified acronym of a sensitive intelligence program. In seconds, the database had provided an article from a reputable publication that described the project in detail. Nothing prevents a hostile intelligence service, terrorist group, or deranged individual from entering the name of a suspected covert employee and discovering that he or she, according to such and such article, previously was an alleged spy in X country.

Because of such continuing threats, the IIPA's Section 421(c) should be amended to:

- Excise the clause that an individual has to be involved in a pattern of activities intended to expose covert identities.
- Remove the *mens rea* standard that the violator has to have reason to believe such actions would impair US intelligence activities and thus reduce the offense to one of strict liability.
- Apply the Act to those who purport to reveal identities in addition to those who disclose actual

identities.

Furthermore, the definition of "covert agent" under Section 426(4)(a) should be revised to omit the requirement that an intelligence officer must have served outside the United States within the past five years to qualify for protection under the Act. Congress also should explicitly state that the statute is universally applicable and that no segment of the population, be it the media or otherwise, is immune from prosecution for revealing identities. Finally, the applicable fine should be increased, perhaps to $50,000.

If such proposals were adopted, Section 421(c) could read:

> *Whoever discloses any information that identifies or purports to identify a covert agent to any individual not authorized to receive classified information shall be fined not more than $50,000 or imprisoned not more than three years, or both.*

While such a revision would expand the scope of Section 421(c) beyond IIPA's original apparent intent, it would greatly enhance protection of the identities of US intelligence officers. Removing the requirement of a "pattern" of activities would mean that any instance an identity is revealed or purported to be revealed, regardless of how it was obtained, would be actionable.

Terminating the "with reason to believe" *mens rea* burden would end arguments regarding subjective versus objective standards and would refine the crime to one of strict liability: either the identity was disclosed or purported to be disclosed, or it was not. Mistake of fact therefore would not be a defense because the augmented statute would proscribe the act of claiming to identify covert agents rather than just the more limited act of actually identifying a covert agent. While strict liability for a felony is not common to most criminal infractions, it is present in public safety measures (worker safety and automobile speeding) and the protection of minors (selling alcohol to underage individuals and statutory rape). Pursuant to *United States v. Balint* (258 U.S. 250 [1922]), strict liability is constitutional so long as its existence is made clear by Congress.

Expanding Section 421(c) to cover both individuals who actually expose identities and those who only purport to disclose identities is crucial to tightening up Section 421(c)'s procedural loopholes. When the statute applies to those who claim to reveal identities, regardless of the accuracy of the information, the IC is not forced into confirming the identity. The offense is boiled down to a simple question: did or did not the individual intend to disclose an identity? There would be no examination of CIPA, the constitutional implications of clearing defense counsel or secret courts, or instructing judges to penalize jurors for talking outside the courtroom after the case ends. If the author actually reveals an identity but claims that his work is fictional, the exercise could return to these complications. The number of instances where this occurs, however, should be quite small because presumably no media member would claim that his work product is fictional.

A necessary corollary to revising Section 421(c) is the removal of Section 422(b), which protected those who have not had access to classified information and who did not engage in a pattern of activities intended to identify and expose covert agents from prosecution for conspiring to violate Section 421(c).

The IIPA's definitions under Section 426 artificially limit the Act's protection to the five-year period following an officer's last foreign duty. Yet identification of an officer much later in life still endangers sources and methods. In addition, as former covert officers may live overseas after leaving the CIA, identification later still could substantially disrupt the former officer's current lifestyle. If Congress insisted on a time limit, more reasonable substitutes could be :

- Protecting the identity as long as the officer either remains under cover or has periods of cover time in his history.
- Extending the five-year limit to 25 years.
- Starting the five-year, or perhaps 15-year, clock after the officer ends employment with US

intelligence.

Finally, to erase the boundaries created by legislative intent under the IIPA, Congress should explicitly state that its sense is that the IIPA be applied universally and that no particular US citizen be immune from prosecution under the IIPA. The Act still would not cover disclosures authorized by the appropriate representative of the executive branch or by the covert agents themselves. If Congress felt it necessary, it could extend this authority to the chairs of the intelligence oversight committees, although this would be at odds with the position taken by the executive branch on classified information.

There is a strong argument that a strengthened IIPA would not violate the First Amendment. Holmes's eloquent yet concise exposition on free speech and the Constitution in *Schenk v. United States* (249 U.S. 47 [1919]) applies as much today as did in 1919, when it was handed down:

> *The most stringent protection of free speech would not protect a man in falsely shouting fire in a theater and causing a panic. It does not even protect a man from an injunction against uttering words that may have all the effect of force. . . . The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree. When a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no court could regard them as protected by any constitutional right.*

A Question of Trust

Perhaps a 15th anniversary initially may seem a subjective benchmark to use to advocate amending the IIPA. In recent years, however, a host of attacks targeting official Americans has occurred, and cover mechanisms are being challenged as never before. Without a precipitating tragedy such as Richard Welch's death to serve as a rallying cry, there is little bureaucratic incentive to push for Congressional change. Nonetheless, the United States should be morally obligated to do its best to safeguard its covert operatives in their unique endeavors. To do less would be to abrogate the trust that our officers, sources, and assets place in the United States to protect them.

Notes

1. Remarks by former President Bush at CIA Headquarters (Retirees Day), Public Affairs Staff, CIA.

2. "Secrecy, "Dirty Tricks" at Heart of CIA Battle," *U.S. News & World Report*, 12 January 1976.

3. Steven V. Roberts. "Greeks' Search for Killers of CIA Man Unfruitful," *The New York Times*, 25 December 1975.

4. Laurence Stern. "Welch Death May Figure in Hill Battle," *The Washington Post*, 29 December 1975.

5. News Briefs, *The Wall Street Journal*, 29 December 1975, p. 1A.

6. Although the CIA is not the sole part of the US Government that sends clandestine intelligence officers overseas, for purposes of this paper, officers will be referred to exclusively as from the CIA. See "Testimony, March 6, 1996, Harold Brown, Chairman, Commission on the roles and Capabilities of the US Intelligence Community, House Permanent Select Committee on Intelligence," *Federal Document Clearing House Congressional Testimony*, 6 March 1996, disseminated electronically via LEXIS/NEXIS.

7. J. F. terHorst. "Lists of U.S. Agents Abroad Abound," *Detroit News*, 7 January 1976.

8. Smith Hempstone. "Our Times," via original dissemination, 6 January 1976.

9. "Greek Committee Reveals the CIA Menace in Athens," *Athens News* 25 November 1975.

10. "Intelligence Identities Protection Act of 1981," United States Senate, Committee on the Judiciary, Report No. 97-2-1, 6 October 1981.

11. "U.S. Aides Called Spies, Ousted," *Facts on File World News Digest*, 13 March 1981. Electronically disseminated via LEXIS/NEXIS. See also: William J.Casey, "Statement for the Record for the House Permanent Select Committee on Intelligence, Subcommittee on Legislation on 7 April 1981."

12. "U.S. Diplomats Expelled," *Facts on File World News Digest*, 3 July 1981, electronic dissemination via LEXIS/ NEXIS. See also: Carlye Murphy. "U.S. Disputes Spy Allegation by Mozambique," *The Washington Post*, 6 March 1981, p. A24.

13. Ronald Reagan. "Remarks of the President at Bill Signing Ceremony at CIA Headquarters," press release, Office of the Press Secretary, The White House, 23 June 1982.

14. Judith Schenk Koffler and Bennett L Gershman. "National Security and Civil Liberties: The New Seditious Libel," *69 Cornell L. Rev. 816*, April 1984. See also: Susan D Charkes. "The Constitutionality of the Intelligence Identities Protection Act," 83 Colum. L. Rev. 727, April 1983.

15. Blaine Harden. "Ghana Mixes Capitalism, Radical Foreign Policy," *The Washington Post*, 24 August 1986, p. A24.

16. "Defendant in Spy Case Tells Why He Sold Secrets to Soviet Officials," *The New York Times*, 10 April 1986, p. A15.

17. CIA Clerk Pleads Guilty in Leaks," *Chicago Tribune*, 14 August 1985, p. 8. See also: "Woman Admits Two Counts of Spying," *The Bergen Record Associated Press*, 13 August 1985, p. A05

18. Richard Norton-Taylor. "Sex and the Unemployed Spy," *The Guardian*, 27 May 1995, p. 23.

19. "Ex-Marine May Wed Lover in Spy Scandal," *The Arizona Republic*, 25 December 1994, p. A36.

20. Robert C. Toth. "CIA Critic Agee Reportedly Paid by Cuba," *The Los Angeles Times*, 10 August 1992, p. A1.

21. James Risen. "Once Again, Ex-Agent Agee Eludes Grasp of the CIA," *The Los Angeles Times*, 14 October 1997, p. A1.

22. 50 U.S.C.A. 421 (c).

23. Report of the Senate Committee on the Judiciary on the Intelligence Identities Protection Act of 1980, 24 September 1980, pp. 15, 17.

24. Statement of Senator Chafee on S.2216 before the Senate Committee on the Judiciary, 5 September 1980, pp. 2, 7.

25. Conference Report of the House-Senate Conference Committee on the Intelligence Identities Protection Act, 20 May 1982, p. 8.

26. "FY 1997 Intelligence Authorization Act (Conference Report)," Congressional Press Release, *Federal Document Clearing House, Inc.*, 24 September 1996.

27. 18 U.S.C.A. App.

28. 28. 15 U.S.C. selections 1801-1809

29. Executive Order 12949, 19 February 1995. See also: Jim Wolf. "Judge Grants Singapore Trip," *Reuters North American Wire*, 14 February 1997. Distributed electronically via LEXIS/NEXIS.

30. "Security Procedures Established Pursuant to Pub. L. No. 95-511, 91 Stat. 1783, by the Chief Justice of the United States for the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review." (1978). See also: Royce Lamberth. "Intelligence on the FISA Court," *Legal Times*, 14 April 1997, p. 18.

31. Royce Lambeth. "Intelligence on the FISA Court," *Legal Times*, 14 April 1997.

32. Leonard Doyle. "The Cold Killers of 17 November Who Always Go Free," *The Guardian* (London), 28 September 1997, p. 14.

(b)(3)(c) was a law clerk with CIA's Office of General Counsel while attending Stanford Law School.

Unclassified

Next Previous Contents